

#3

EJ 874 818 156 US

Attorney Docket No.:47225

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the patent application of:

Shoichi Kiyomoto

Serial No.: Not yet known

Filed: January 22, 2001

Title: METHOD OF SECURELY TRANSMITTING INFORMATION



INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In compliance with 37 CFR §§ 1.97 and 1.98, Applicant brings to the attention of the U.S. Patent and Trademark Office information listed on the enclosed Information Disclosure Statement form. Except as noted below, a copy of the information is also enclosed.

Concise explanations of non-English language information listed on the enclosed Information Disclosure Statement Form are set forth in the abstracts and summaries provided on the attached pages.

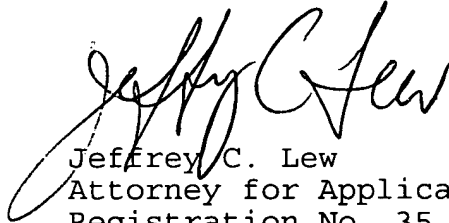
Reference A302 is a Japanese language book, the pertinent portions of which are summarized in the attachments. Therefore, Applicant has not provided a copy of the Japanese language text. Applicant will be pleased to provide a copy if the Examiner requests.

Applicant calls attention to the fact that Japanese patent applications Nos. 10-356681 and 11-0053728 are referenced on

pages 5, 6 and 9 of the application with respect to disclosures contained respectively therein. Applicant now wishes to clarify that these Japanese patent applications were withdrawn prior to publication. Therefore, they are not listed in the enclosed Information Disclosure Statement and copies/translations (other than summaries recited in the specification) are not included herewith.

It is respectfully requested that the Examiner initial the enclosed Information Disclosure Statement Form upon consideration of the cited documents and return an initialed copy with the next correspondence.

Respectfully submitted,



Date: January 22, 2001
1403 Silverside Road
Wilmington DE 19810
Facsimile: (302) 475-7915

Jeffrey C. Lew
Attorney for Applicant
Registration No. 35,935
Telephone: (302) 475-7919

Japanese Kokai Patent Publication No. 9-274431

Titled: Method of securing computer data

Abstract: This invention provides a method and an apparatus which enables an administrator, who manages deposited confidential information, to prevent transferring the data to a person who does not have the right to receive the data.

This invention defines an encrypted password data and deposited record of self-identification data of a true owner/client in a definition phase by using an arbitrary identification/definition phase and search phase of confidential information right after purchasing a computer. A user inputs his/her unique password or a series of information, and then voluntarily deposits another confidential information for search. Identification mark is linked with the confidential information (such as a user's encrypted password), and encrypted with the administrator's public key. After entering a unique individual identification, the user selects a password to protect his/her system. All individual identification data with the password are encrypted with the public key of the administrator and then stored into the user's computer as the deposited confidential protection record. The password is used to encrypt all data on a user's disk.

Japanese Kokai Patent Publication No. 8-171535

Titled: Record regeneration apparatus, method of record regeneration, transmission/reception apparatus, and method of transmission/reception

Abstract: This invention almost completely secures personal information for a record regeneration apparatus, and discloses a method of record regeneration, a transmission/ reception apparatus, and a method of transmission/ reception.

This invention almost completely secures information of an individual by making a common key in a predetermined format utilizing fingerprint and voiceprint data and encrypting and then decrypting the information with the common key. This invention may prevent the encrypted information from being read, and thus may secure the confidential information of the individual. This invention also prevents interception of the information by a third party while the information is being transmitted after encrypting the information with a common key which is constructed with fingerprint and voice data of the individual, and then decrypting the received information with the common key. In this way, the security of personal information is protected while being transmitted and received by the transmission/reception apparatuses and method.

Kokai No. 11-282983

Titled: Self -identification by Fingerprint Data

This invention provides a sure self-identification method utilizing an IC card which has small memory capacity for storing Fingerprint information.

Abstract: When the IC card stores its owner's fingerprint data 6 which were input beforehand, the fingerprint data was encoded with the process 1, a redundant data 2 were generated, and redundancy addition 3 was performed. Furthermore, the digitized information to be stored was compressed to less than 1/3 of its original capacity by encryption 4 with the key 5 of the true owner. When this IC card is used, it is inserted into a card reader while the user inputs his/her fingerprint 13. The acquired fingerprint data 7 from the user is used to obtain the redundant data based on the user's fingerprint by generating the redundant data 8. The signal from the IC card is performed the decryption 9 with the user's key 12 so that the redundant data 10 may be extracted, compared with the redundant data for the newly input fingerprint. In this way it is possible to determine whether both redundant data are the same or not.

Computer Image Process (Application Vol. 3, October 10, 1992, published by Soken Shuppan, Co., Ltd.)

The pertinent portion of this reference is summarized at page 5, lines 1-7 of the specification which is reproduced as follows:

each gray-scaled pixel of a digitized fingerprint image is binary-coded (black or white);

either the ridge (the black pixel line) or the valley (the white pixel line) is narrowed down to the width of a single pixel size;

the directions of either the ridge or the valley of the previous step are calculated using all pixel points of the fingerprint image; and

the above narrowed-down information is correlated with the directions determined in the previous step.

Open Design NO. 14 (1996) *"Implementation of Security by Advanced Encryption Technology"* published by CQ Publication Co., Ltd. (Japan)

The pertinent portion of this reference describes the Boolean algebra operation which is summarized in detail from page 11, line 1 through page 12, line 8 of the specification, reproduced, below.

One preferred and simple encryption method using the "fingerprint information" as the key is to perform an Boolean algebra "exclusive OR" operation on each bit of the plain text {D} and the binary data of the digital encoding key generated by the group of minutia from fingerprint information.

The well known Boolean algebra exclusive OR operation, sometimes referred to as "XOR", with respect to two binary data sets A and B may be summarize in Table III, as follows:

Table III

Data value of bit in set A	Data value of bit in set B	Result of exclusive OR operation (A XOR B)
1	0	1
0	1	1
1	1	0
0	0	0

The bits of binary data from the minutiae of a fingerprint and Plain text {D} may be considered to correspond to A and B, respectively, and the exclusive OR operation of Table III can then be performed on each bit of plain text with the corresponding sequential bit of binary data from the minutia. This product of the XOR operation is a string of binary bits containing the plain text information encoded by the binary data from the minutia. The encrypted plain text information is not understandable in the encoded form but can be decoded to intelligible form by reversing the XOR operation, provided, of course, that the decoding entity has access to the original coding key of binary data from the minutia.

By way of simple example of the application of the exclusive OR operation to produce encoded information, assume that the binary data {FD} of the minutiae and the plain text {D} form 4 bit binary codes:

$\{FD\} = \{1, 0, 0, 1\}$; and

$\{D\} = \{1, 1, 0, 0\}$.

The plain text $\{D\}$ may be encrypted with the key $\{FD\}$ applying the exclusive OR operation on each bit to obtain the XOR encrypted binary data set:

$\{\underline{D}\} = \{0, 1, 0, 1\}$.

This encrypted text $\{\underline{D}\}$ can be decrypted by re-applying the exclusive OR operation between $\{\underline{D}\}$ and $\{FD\}$:

$\{D'\} = \{1, 1, 0, 0\}$

The decrypted text $\{D'\}$ is identical to $\{D\}$ because the decryption with the exclusive OR operation is reversible.